

### REMARKS

In response to the Final Office Action mailed July 11, 2008, Applicants respectfully request reconsideration and entry of this amendment. To further the prosecution of this application, amendments have been made in the claims, and each of the rejections set forth in the Office Action has been carefully considered.

Claims 1-42 were previously pending in this application. By this amendment, claims 1, 3, 6, 7, 9, 12, 21, 23, 26, 27, 29 and 41 have been amended. Claims 5, 8, 25, and 28 have been canceled without prejudice or disclaimer. No new claims have been added. As a result, claims 1-4, 6, 7, 9-24, 26, 27, and 29-42 are pending for examination, with claims 1, 14, 21, 34, 41, and 42 being independent. No new matter has been added.

#### Amendments to the Claims

Applicants request that the amendments be entered to expedite prosecution of this application. In addition to minor clarifications made to claims 1, 21, and 41, the amendments incorporate limitations previously recited in at least one other previously pending claim. Therefore, these amendments should not be regarded as raising new issues.

#### Telephone Conference with the Examiner

Initially, Applicants' representative thanks Examiner Zia for the courtesies extended in granting and conducting a telephone interview on August 26, 2008, the substance of which is summarized herein. Applicants were represented at the interview by the undersigned. Technology Specialist Zachary Thomas also participated in the call.

During the telephone interview, Applicants' representative initially provided an overview of some embodiments of the invention. Differences between the claims and Nyman reference were also discussed. The amendments and remarks herein may serve as a further summary of the interview.

#### Brief Description of Some Embodiments

The present application relates to a peer-to-peer collaboration system [01]. In such a peer-to-peer collaboration system, encryption keys that can be used to transmit information securely are exchanged between collaboration members [53]. However, one way that security may be defeated

is if a user is “spoofed” into thinking that he or she is communicating with an authorized user, when in fact he or she is communicating with an unauthorized user [54]. This scenario may occur, for example, if the unauthorized user attempts to join the peer-to-peer collaboration session using a display name that is equivalent to the display name of the authorized user [62]. One of the collaborating users may mistakenly communicate with the unauthorized user.

To avoid such a breach of security in a peer-to-peer collaboration system, the present application describes that when the peer-to-peer collaboration system offers a user an opportunity to select a contact with which to communicate, the system displays relevant status information about contacts to be selected. For example, the display provided by the system may include information about whether the contact has been authenticated or certified. The specific actions that may be allowed or disallowed may be specified in a security policy [82-85]. Fig. 12 is flowchart of a process through which the security policies may be applied in practice [119-127]. A security policy may restrict communication or warn a user of an attempt to communicate with a contact that would violate the security policy, which creates an option for the user to choose whether to continue with the communication [127].

#### Rejections under 35 U.S.C. §102

The Office Action rejected claims 1-42 under 35 U.S.C. §102(e) as being anticipated U.S. Patent Application No. 2003/0037033 (Nyman). Applicants respectfully disagree.

#### Claim 1

Claim 1 as amended, is directed to a method for managing and displaying contact authentication in a peer-to-peer collaboration system. By this amendment, limitations from claims 3, 5, and 8 have been incorporated into claim 1. Claim 1 recites “warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level.” Support for this limitation can be found, for example, in FIG. 12 and the accompanying text.

This limitation clearly distinguishes over the cited reference. In Nyman, no such warning is made. The Office Action asserts that this limitation is met by the description in paragraph 94 of Nyman. However, this passage describes encrypting a first user’s name (“MARK”) and alternate name (“MARK’S PC”) with a public key of a second user permitted to display the first user’s name.

Other users' devices are unable to decrypt the user name and does not display it. The other users, therefore, cannot select the first user to attempt to communicate with the first user. Applicants respectfully submit that there is no reasonable interpretation of the claim or reference under which Nyman meets the limitation of "warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level" in conjunction with the other limitations of the claims.

Accordingly, claim 1 patentably distinguishes over the prior art of record, so that the rejection of claim 1 under 35 U.S.C. §102 should be withdrawn.

#### Claims 21 and 41

Independent claims 21 and 41 similarly recite limitations not shown or suggested in Nyman. For example, claim 21 as amended recites "a mechanism that warns a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level."

Independent claim 41 as amended, also recites limitations that distinguish over the reference. For example, claim 41 recites "program code for warning a user based on the security policy when that user attempts to communicate with a contact having a predetermined authentication level."

For reasons that should be apparent from the foregoing discussion of Nyman in connection with claim 1 that the reference does not meet the limitations of these claims.

Accordingly, claims 21 and 41 patentably distinguishes over the prior art of record, so that the rejection of claims 21 and 41 under 35 U.S.C. §102 should be withdrawn.

#### Claim 14

Claim 14 is directed to a method for managing and displaying contact authentication in a peer-to-peer collaboration system wherein users may have multiple authentication and certification levels, including an unauthenticated and uncertified level. Claim 14 recites "presenting on the display information constituting a warning to the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level."

This limitation clearly distinguishes over the cited reference. In Nyman, no such warning is presented on a display to a user. The Office Action asserts that these limitations are met by the

description in paragraphs 27 and 93 of Nyman. However, these passages describe that when a person configures their own device, that person can specify which other user will be able to use their chosen name to display an indication of their device. Applicants respectfully submit that there is no reasonable interpretation of the claim or reference under which Nyman meets the limitation of "presenting on the display information constituting a warning to the user" in conjunction with the other limitations of the claims.

Accordingly, claim 14 patentably distinguishes over the prior art of record, so that the rejection of claim 14 under 35 U.S.C. §102 should be withdrawn.

#### Claims 34 and 42

Independent claims 34 and 42 similarly recite limitations not shown or suggested in Nyman. For example, claim 34 recites "a mechanism that presents on the display information constituting a warning to the user and restricts the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level based on the security policy."

Independent claim 42 also recites limitations that distinguish over the reference. For example, claim 42 recites "program code for presenting on the display information constituting a warning to the user and restricting the user from communicating with the selected contact based on the security policy when the selected contact has an unauthenticated and uncertified level based on the security policy."

For reasons that should be apparent from the foregoing discussion of Nyman in connection with claim 14, the reference does not meet the limitations of these claims.

Accordingly, claims 14 and 42 patentably distinguishes over the prior art of record, so that the rejection of claims 14 and 42 under 35 U.S.C. §102 should be withdrawn.

#### Dependent Claims

The remaining claims depend from one of the independent claims, and should be allowed for at least the same reasons. The dependent claims recite further limitations that distinguish over the reference. Applicant reserves the right to argue for the further patentability of these claims.

**CONCLUSION**

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, the Director is hereby authorized to charge any deficiency or credit any overpayment in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 23/2825, under Docket No. M1103.70263US00.

Dated: October 14, 2008

Respectfully submitted,

By 

Edmund J. Walsh

Registration No.: 32,950

WOLF, GREENFIELD & SACKS, P.C.

Federal Reserve Plaza

600 Atlantic Avenue

Boston, Massachusetts 02210-2206

617.646.8000

x10/11/08x